SOC Analist / Cybersecurity Adviseur

Functieomschrijving

Ben jij gepassioneerd over cybersecurity en wil je een cruciale rol spelen in het beschermen van organisaties tegen cyberdreigingen? Ben je een multidisciplinaire zelfstarter in teamverband die stevig in zijn of haar schoenen staat en zich niet snel het bos in laat sturen?
Bij het Rijksvastgoedbedrijf (RVB) zijn we op zoek naar een gedreven SOC Analist annex Cybersecurity Adviseur die ons team komt versterken. In deze dubbelrol ben jij de eerste lijn van verdediging tegen cyberaanvallen en speel je een sleutelrol in het waarborgen van de digitale veiligheid van onze systemen. Daarnaast geef je gevraagd en ongevraagd technisch inhoudelijke adviezen over cybersecurityvraagstukken, variërend van infra en SDLC tot ICS/IoT.
Ben jij gepassioneerd over cybersecurity en wil je een cruciale rol spelen in het beschermen van organisaties tegen cyberdreigingen? Ben je een multidisciplinaire zelfstarter in teamverband die stevig in zijn of haar schoenen staat en zich niet snel het bos in laat sturen?
Bij het Rijksvastgoedbedrijf (RVB) zijn we op zoek naar een gedreven SOC Analist annex Cybersecurity Adviseur die ons team komt versterken. In deze dubbelrol ben jij de eerste lijn van verdediging tegen cyberaanvallen en speel je een sleutelrol in het waarborgen van de digitale veiligheid van onze systemen. Daarnaast geef je gevraagd en ongevraagd technisch inhoudelijke adviezen over cybersecurityvraagstukken, variërend van infra en SDLC tot ICS/IoT.

Taken en verantwoordelijkheden

Als SOC Analist draai je mee in de continuïteit van monitoring en analyse. Je houdt toezicht op netwerkverkeer, servers, endpoints en applicaties om verdachte activiteiten snel te detecteren. Hierbij maak je gebruik van geavanceerde SIEM-tools zoals Elastic Search en Splunk om real-time analyses uit te voeren. Daarnaast ontwikkel en implementeer je detectieregels en -scripts in Python of PowerShell om bedreigingen effectief te identificeren en te mitigeren.
Naast monitoring speel je een cruciale rol in het incident response proces. Je voert diepgaande technische analyses uit, begeleidt forensische onderzoeken op getroffen systemen en werkt nauw samen met collega’s in het Incident Response Team om snel en adequaat te reageren. Je analyseert malware, identificeert aanvalsvectoren en stelt gedetailleerde rapporten op met bevindingen en aanbevelingen voor preventieve maatregelen. Ook ondersteun je pentesttrajecten tot en met het mitigeren van de bevindingen.
Als Cybersecurity Adviseur geef je technisch inhoudelijk advies op alle securityvraagstukken binnen de RVB, niet alleen op infragebied, maar ook op SDLC (Software Development Life Cycle) en ICS/IoT. Je vertaalt beleidskaders zoals ISO, BIO en NIS2 naar praktische maatregelen en combineert deze met SOC monitoring, incident- en vulnerability management. Initieel richt je je op de IV-keten, maar op termijn zal je verantwoordelijkheid worden uitgebreid naar andere domeinen binnen de RVB.

Daarnaast ben je verantwoordelijk voor:

- Threat Intelligence: het verzamelen en analyseren van informatie over nieuwe en opkomende dreigingen, en up-to-date blijven met de laatste trends en technieken in cyberaanvallen.
- Vulnerability Management: het identificeren, beoordelen en verhelpen van

kwetsbaarheden in systemen en netwerken, inclusief het ondersteunen bij pentesten en het implementeren van oplossingen.
•Verbetering van beveiligingsprocessen: gevraagd en ongevraagd evalueren van bestaande maatregelen en het doen van concrete aanbevelingen voor verbeteringen. Je test, begeleidt en implementeert nieuwe beveiligingstechnologieën en -tools.
•Opleiding en bewustwording: het ondersteunen van trainingen en bewustwordingsprogramma's voor personeel om de algehele beveiliging te verbeteren.
•Samenwerking: het werken met andere IT-, OT- en beveiligingsteams om beveiligingsmaatregelen te verbeteren, en waar nodig samenwerken met externe partners en autoriteiten.

Nieuwsgierig geworden naar de functie van *SOC Analist*, maar wil je inhoudelijk nog wat meer informatie over deze functie? Bel of app René van Erve,Manager Security Services, via 06-15383376.

Wil je meer weten over werken bij het Rijksvastgoedbedrijf? Bekijk dan ook onze pagina **Digitalisering bij het RVB** Hier ontdek je meer over hoe het er bij ons aan toe gaat, de verschillende werkgebieden, disciplines en rollen, verteld door onze echte collega's.

Functie-eisen

Minimaal HBO werk- en denkniveau, met aantoonbare ervaring als SOC-specialist of in security incident management binnen SOC-SIEM omgevingen. Verder breng je kennis mee van:

•Cloud-, IaaS- & VMaaS-omgevingen;
•SIEM-tools (bijv. Elastic, Splunk);
•Aanvalstechnieken en malware;
•IP-netwerkconcepten, monitoring en detectie;
•IoT/OT/gebouwenbeheersystemen is een pré;

En je hebt ervaring met:

•Securitydiensten zoals IDS/IPS en kwetsbaarhedenmanagementsystemen (Nessus);
•Het ontwikkelen van detectieregels en scripts (Python, PowerShell);
•Incident response, begeleiden forensische analyses en malware-analyse;
•Vulnerability management en begeleiden pentesten;
•Input verzorgen voor managementrapportages;
•Beleidskaders zoals ISO, BIO, NIS2, NCSC, NIST, CBW, CRA en CIS, en de vertaling hiervan naar praktische maatregelen.

Naast alle inhoudelijke skills die je meeneemt zijn we ook vooral op zoek naar een teamplayer met een proactieve houding waar ook mee gelachen kan worden!

Bijzonderheden

•De gesprekken staan gepland in week 50 op onze locatie in Den Haag.
•Omdat we duurzaamheid stimuleren, reizen we zoveel mogelijk met het openbaar vervoer. Je krijgt daarom van ons een ov-kaart voor woon-werkverkeer en dienstreizen. Voor locaties die niet goed te bereiken zijn met het ov zijn bedrijfsauto's beschikbaar.
•Bij het Rijksvastgoedbedrijf werken we onafhankelijk van tijd, plaats en apparaat. Je overlegt met jouw leidinggevende hoe je hier invulling aan geeft. Het kan dus ook zijn dat je af en toe op een andere locatie of thuis werkt.

Klik hier als je nieuwsgierig bent naar wat het Rijksvastgoedbedrijf jou te bieden heeft.
Een veiligheidsonderzoek kan deel uitmaken van de procedure. We gaan ervan uit dat je bereid bent om daaraan mee te werken. Hier vind je meer informatie daarover.
Binnen de Rijksoverheid werken we met raamovereenkomsten voor de inhuur van personeel. Acquisitie naar aanleiding van deze vacature wordt daarom niet in behandeling genomen.

Meer over jouw toekomstige afdeling

Directie Strategie en Digitalisering

De volledige I-functie van het Rijksvastgoedbedrijf is ondergebracht bij de directie S&D. Wij verbinden departementen, beleidsmakers, vastgoedhoudende diensten, medeoverheden en maatschappelijke organisaties met het Rijksvastgoedbedrijf op strategisch niveau. De vastgoedportefeuille van het Rijksvastgoedbedrijf is daarbij leidend. De afdeling Informatieservices is onderdeel van de directie S&D.

Afdeling Informatie Voorziening

Binnen de directie S&D is de afdeling Informatie Voorziening (IV) met 160 medewerkers verantwoordelijk voor de ontwikkeling en de levering van de informatiediensten. De functie van SOC Analist zit in de sectie Security Services, team Cyber security center dat onderdeel is van de afdeling IV. De sectie Security Services is verantwoordelijk voor:

- Het Cybersecuritycenter dat monitoring, kwetsbaarheden scanning en incidentmanagement diensten levert
- Het team Hoog Beveiligd dat IV diensten in het hoog beveiligde domein levert

Dit bieden we nog meer

Bij het RVB werk je aan het fundament van Nederland. Om dat werk goed en met vakmanschap te kunnen doen, krijg je ruimte om je te ontwikkelen, werk en privé goed te combineren en keuzes te maken in je arbeidsvoorwaarden.

- **Extra budget en tijd.** Je krijgt een Individueel Keuzebudget (IKB): 16,5% van je salaris en jaarlijks 64 IKB-uren bij een werkweek van 36 uur. De vakantie-uitkering van 8% zit in het IKB-budget. Je kunt het laten uitbetalen of gebruiken voor bijvoorbeeld extra verlof, een fiets, je studieschuld of verduurzaming van je woning.
- **Vakantie en Verlof.** Bij een werkweek van 36 uur krijg je jaarlijks 144 vakantie-uren. Daarnaast zijn er verschillende verlofregelingen. Zo kun je betaald ouderschapsverlof opnemen met 75% tot 100% doorbetaling en onbetaald ouderschapsverlof tot je kind 8 jaar is.
- **Reizen en Thuiswerken.** Je woon-werkverkeer met het openbaar vervoer wordt volledig vergoed. Reis je met eigen vervoer, dan kun je afhankelijk van je situatie een kilometervergoeding krijgen. Voor thuiswerken zijn er een vergoeding en voorzieningen voor een goede werkplek.
- **Ontwikkeling.** Via de RVB Academie kun je trainingen en workshops volgen. Ook kun je met je leidinggevende bespreken welke externe opleiding, cursus of certificering bij je ontwikkeling past.
- **Pensioen.** Je bouwt pensioen op bij ABP, waarbij het RVB meebetaalt aan je pensioenpremie.

Meer weten? Lees op de pagina **"Dit bieden we jou bij het RVB"** meer over onze arbeidsvoorwaarden en ontwikkelmogelijkheden.